Dandelion: Privacy-Preserving Transaction Propagation in Bitcoin’s P2P Network

Presenter: Giulia Fanti

Joint work with: Shaileshh Bojja Venkatakrishnan, Surya Bakshi, Brad Denby, Shruti Bhargava, Andrew Miller, Pramod Viswanath
Bitcoin P2P Primer

Blockchain
sd93fjj2
pckrn29
...
trx
Privacy requirement:

Address and real identity must be unlinkable
Today, messages spread with diffusion.
Diffusion is vulnerable to source detection!

Biryukov et al. CCS 2014
Koshy et al., Financial Crypto 2014
F. and Viswanath, NIPS 2017
Dandelion

Lightweight transaction propagation algorithm with provable privacy guarantees.

Venkatakrishan et al., ACM Sigmetrics 2017; F. et al., ACM Sigmetrics 2018
FAQ: Why not alternative solutions?

Connect through Tor

I2P Integration (e.g. Monero)
Model

Assumptions and Notation
Adversarial model

- Spies collude
- Observe all metadata
- Identities unknown
- Fraction $p$ of spies
- Honest-but-curious
Metric for Anonymity

Recall

\[ \frac{1}{n} \sum_{v} 1\{M(v's \text{ tx}) = v\} \]

Precision

\[ \frac{1}{n} \sum_{v} \frac{1\{M(v's \text{ tx}) = v\}}{\# \text{ tx mapped to } v} \]
Goal:

Design a distributed flooding protocol that minimizes the maximum precision and recall achievable by a computationally-unbounded adversary.
Fundamental Limits

**Thm**: Maximum recall $\geq p$.

**Thm**: Maximum precision $\geq p^2$. 

Fraction of spies
What are we looking for?

Asymmetry

Mixing

1 2 3 4 spy
What can we control?

- Spreading Protocol
  - Given a graph, how do we spread content?
  - Diffusion

- Topology
  - What is the underlying graph topology?
  - Approximately regular

- Dynamicity
  - How often does the graph change?
  - Dynamic
  - Static
Spreading Protocol: Dandelion

1) Anonymity Phase

2) Spreading Phase
Theorem: Dandelion spreading has an optimally low maximum recall of $p + O\left(\frac{1}{n}\right)$.

lower bound = $p$

fraction of spies

number of nodes
Graph Topology: Line

Anonymity graph

“Regular” graph

tx1

tx2
Dynamicity: High

Change the anonymity graph frequently.
DANDELION Network Policy

Spreading Protocol

Topology

Dynamicity

Given a graph, how do we spread content?

What is the anonymity graph topology?

How often does the graph change?

Dandelion Spreading

Line graph

Dynamic

Static

19
Theorem: DANDELION has a nearly-optimal maximum precision of \( \frac{2p^2}{1-p} \log \left( \frac{2}{p} \right) + O \left( \frac{1}{n} \right). \)*

*For \( p < \frac{1}{3} \)
Performance: Achievable Region

![Diagram showing the achievable region for precision and recall with points labeled as Flooding, Diffusion, and DANDELION.]
Why does DANDELION work?

Strong mixing properties.

Tree

Too many leaves

Precision: $\theta(p)$

Complete graph (Crowds, Tor)

Too many paths

Precision: $\frac{p}{1-p} (1 - e^{p-1})$
Graph construction in practice

Choose $d=1$ outbound edges
Gives approximate $d$-regular anonymity graph
What are drawbacks of Dandelion?

<table>
<thead>
<tr>
<th>Attack</th>
<th>Effect on Dandelion</th>
<th>Proposed Solution</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graph Learning</td>
<td>Precision increases to $O(p)$</td>
<td>4-regular anonymity graph</td>
<td>Limits precision gain (Thm. 1)</td>
</tr>
<tr>
<td>Intersection</td>
<td>Empirical precision increase</td>
<td>Pseudorandom forwarding</td>
<td>Improved robustness (Thm. 2)</td>
</tr>
<tr>
<td>Graph construction</td>
<td>Empirical precision increase</td>
<td>Non-interactive construction</td>
<td>Reduced precision gain</td>
</tr>
<tr>
<td>Black hole</td>
<td>Transactions do not propagate</td>
<td>Random stem timers</td>
<td>Provides robustness (Prop. 3)</td>
</tr>
<tr>
<td>Partial deployment</td>
<td>Arbitrary recall increase</td>
<td>Blind stem selection</td>
<td>Reduces recall (Thm. 3)</td>
</tr>
</tbody>
</table>

Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees, ACM Sigmetrics 2018
Experiments on mainnet
Take-Home Messages

1) Bitcoin’s P2P network has weak anonymity protections

2) DANDELION may be a lightweight solution against large-scale deanonymization attacks (but doesn’t replace Tor!)

3) More information at:

   https://github.com/dandelion-org/bips
   https://github.com/dandelion-org/bitcoin
Simulation on Bitcoin P2P Topology

![Graph showing probability of detection vs. supernode connections per node with legends for Trickle, Simulated, Trickle, Theoretical lower bound (d=2), Diffusion, Theoretical, and Diffusion, Simulation]

F. and Viswanath, NIPS 2017
4-Regular Graphs

- More robust against adversaries that learn the graph
- Per-transaction routing vulnerable to intersection attacks

- **Pro**: Increases cost of graph-learning attacks
- **Con**: Can make transactions from the same source easier to link
FAQ: Why not Tor?

- Tor, VPNs, etc. address this problem

- Only work for savvy or privacy-aware users

- If Bitcoin is to become a mainstream payment system, it should protect everyone’s transactions

- Dandelion: lightweight, easy to integrate into existing network
Moving from theory to practice
Implementation: Dandelion spreading

1) Anonymity Phase

2) Spreading Phase
Anonymity graph construction
Adversarial Model: Byzantine nodes

Learn the graph

Misbehave during graph construction

Misbehave during propagation

4-regular graphs
Anonymity graph construction
Dealing with stronger adversaries

Learn the graph

Misbehave during graph construction

Misbehave during propagation

4-regular graphs

Only send messages on outgoing edges

Multiple nodes diffuse
Partial deployment

Running Dandelion

Not running Dandelion

tx1
Latency Overhead: Estimate

Time to first transaction sighting (s)
DANDELION vs. Tor, Crowds, etc.

1) Messages propagate over the same cycle graph.

2) Anonymity graph changes dynamically.

3) No encryption required.
d-regular graphs give robustness!
Anonymity graph construction

Base Case

$k=1$ rounds of Degree-Checking

Base Case

$k=1$ Rounds

Degree
Dealing with stronger adversaries

- Learn the graph
- Misbehave during graph construction
- Misbehave during propagation

- 4-regular graphs
- Get rid of degree-checking
- Multiple nodes diffuse
Learning the anonymity graph

<table>
<thead>
<tr>
<th></th>
<th>Line</th>
<th>Random regular</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precision</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graph unknown</td>
<td>$O\left(p^2\log\left(\frac{1}{p}\right)\right)$</td>
<td></td>
</tr>
<tr>
<td>Graph known</td>
<td>$\Omega(p)$</td>
<td>?</td>
</tr>
</tbody>
</table>
Manipulating the anonymity graph
DANDELION++ Network Policy

Spreading Protocol

Given a graph, how do we spread content?

Topology

What is the anonymity graph topology?

Dynamicity

How often does the graph change?

Dandelion Spreading

4-regular graph

Dynamic

Static